March 1, 2010
**Via ECFS**

Ms. Marlene H. Dortch, FCC Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

**RE: EB Docket No. 06-36**
**Annual 64.2009(e) CPNI Certification for 2009**
**Interface Security Systems Holdings, Inc. Filer ID 827355**

Dear Ms. Dortch:

Enclosed for filing is the 2009 CPNI Compliance Certification submitted on behalf of Interface Security Systems Holdings, Inc. This filing is submitted pursuant to 47 C.F.R. Section 64.2009(e) and in accordance with the Public Notice DA 10-91 issued January 15, 2010.

Any questions you may have concerning this filing may be directed to me at 470-740-3005 or via email to mbyrnes@tminc.com.

Sincerely,

Monique Byrnes
Consultant to Interface Security Systems Holdings, Inc.

Attachments

cc: Best Copy and Printing (via email to FCC@BCPIWEB.COM)
R. House, Interface SS
file: Interface SS – FCC CPNI
tms: FCCx2010-1

**ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

**EB DOCKET 06-36**

| | |
|---|---|
| Annual 64.2009(e) CPNI Certification for : | Calendar Year 2009 |
| Companies covered by this certification: | |
| **Interface Security Systems Holdings, Inc.** | **499 Filer ID 827355** |
| Date Filed: | March 1, 2010 |
| Name of Signatory: | Daniel Reynolds |
| Title of Signatory: | Vice President – Customer Operations |

I, Daniel Reynolds, certify and state that:

1. I am Vice President-Customer Operations for Interface Security Systems Holdings, Inc. and, acting as an agent of the companies, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules *See* 47 C.F.R. § 64.2001 *et seq.*

2. Attached to this certification ,as Exhibit A, is an accompanying statement explaining how the companies procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in Section 64.2001 *et seq.* of the Commission's rules.

3. The companies have not taken any actions (i.e., proceedings instituted or petitions filed by the company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

4. The companies have not received any customer complaints in the past year concerning the unauthorized release of CPNI.

5. The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Daniel Reynolds
Vice President – Customer Operations
2/23/10
Date

Attachments: Accompanying Statement explaining CPNI procedures – Attachment A
Explanation of actions taken against data brokers – not applicable
Summary of customer complaints – not applicable

Attachment A
Statement of CPNI Procedures and Compliance

**Interface Security Systems Holdings, Inc.**

Calendar Year 2009

**ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

**EB DOCKET 06-36**

Interface Security Systems Holdings, Inc.

Statement of CPNI Procedures and Compliance (2009)

Interface Security Systems Holdings, Inc. ("ISS" or "Company") provides digital voice (VoIP) and broadband services to business and residential customers to enhance the company's core business of IP-based electronic security systems. Services are provided on a resale basis. ISS does not have access to, use or permit access to CPNI for sales and marketing of any services outside of the total service approach as specified in 47 CFR §64.2005. If the Company elects to use CPNI in a manner that does require customer approval, it will follow the applicable rules set forth in 47 CFR Subpart U, including institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

ISS receives call detail from its underlying carrier providers by customer account number. This information is used only minimally for customer billing, as customer bills do not include call detail. Access to this information is limited to select Company individuals who receive CPNI training annually, for accounts payable purposes.

Customer CPNI is documented and maintained off site within the databases of our underlying carriers. Upon service initiation, including a complete and executable contract, the Company initiates a computer toolbar with a generic password for initial customer access. Information regarding login for the toolbar is provided to the individual customer who signed the Company service contract. The first customer login drives the customer to select a password. Neither the Company nor its underlying carriers have access to the customer-selected password.

The company utilizes the underlying carrier services of two separate providers and has internal processes for working with both. For operations utilizing the underlying carrier services of one of the underlying carrier providers, ISS employees do not have access to CPNI. If a customer requests access to their proprietary network information they are first directed to the secured web portal or toolbar, which requires the user name and password. If a customer encounters any issues trying to retrieve their CDR (Call Detail Records) they call in to the ISS Helpdesk. The ISS Helpdesk then connects the customer to our underlying VOIP carrier's technical support department who will mail the customer-requested information to their address of record. For operations utilizing the underlying carrier services of the second carrier, ISS employees have access to CPNI through the underlying VOIP carrier's secure web site. This access is limited to the ISS Provisioning and Helpdesk teams. Those ISS employees with such access are trained annually on how to handle and secure CPNI. If a customer requests information or details regarding their CDRs, ISS would first direct them to their web portal which is secured and maintained by the underlying VOIP carrier. If a customer needs a copy of their CDR, ISS does not discuss this matter by phone but mail the CDR to their address of record.

The Company's website includes a bill payment function. Customers cannot view CPNI via this website. Customers enter the Company account number and then payment information. Invoice copies, invoice details, call detail, or network configuration information is not available through this web portal.

For both residential and business customers, the Company's VoIP underlying carriers provide notification to customers via U.S. mail and/or email to the customer's address (email) of record whenever client information is changed. This includes changes of address or telephone number or other basic customer account information.

Company employees with access to CPNI and call detail are trained regarding CPNI protection. Training includes information on what CPNI is and on protection measures. Training refresher is provided on an annual basis. Training includes disciplinary actions and procedures in the event of unauthorized release of CPNI.

The Company does not have any retail locations and therefore does not disclose CPNI at in-store locations.

Requests for call detail records by law enforcement agencies are only granted if a subpoena is provided. Procedures are in place to ensure that the U.S. Secret Service and FBI are notified of breaches of CPNI in accordance with the rules. Although the Company did not have any breaches of CPNI or call detail in 2009, the Company has procedures in place to maintain appropriate records in such an event, and in accordance with FCC rules.

The Company has not taken any actions against data brokers in the last year.

The Company did not receive any customer complaints about the unauthorized release of CPNI or call records in calendar year 2009.

The Company has not developed any information with respect to the processes pretexters are using to attempt to access CPNI or call records.